Introduction to Pen Testing and Open Source Intelligence

Cybersecurity

Penetration Testing Day 1

Class Objectives

By the end of today's class, you will be able to:

- Understand the role of a pentester in assessing a business's security.
- Do reconnaissance on a target network by performing basic DNS enumeration with WHOIS record information.
- Gather domain information using OSINT techniques and tools like Google dorking, Shodan, and certificate transparency.
- Use Shodan and Recon-ng to discover domain server information.

We’ve covered a wide range of cyberattacks and vulnerabilities throughout the course so far.

Now we will look at a specific profession that partners with organizations to assess their security posture, vulnerabilities, and susceptibility to attacks.

(Source)

Today's Class

Today we will cover the following topics:

01

An **introduction** to pen testing and its business goals.

02

A **high-level overview** of the various stages of a pentest engagement.

03

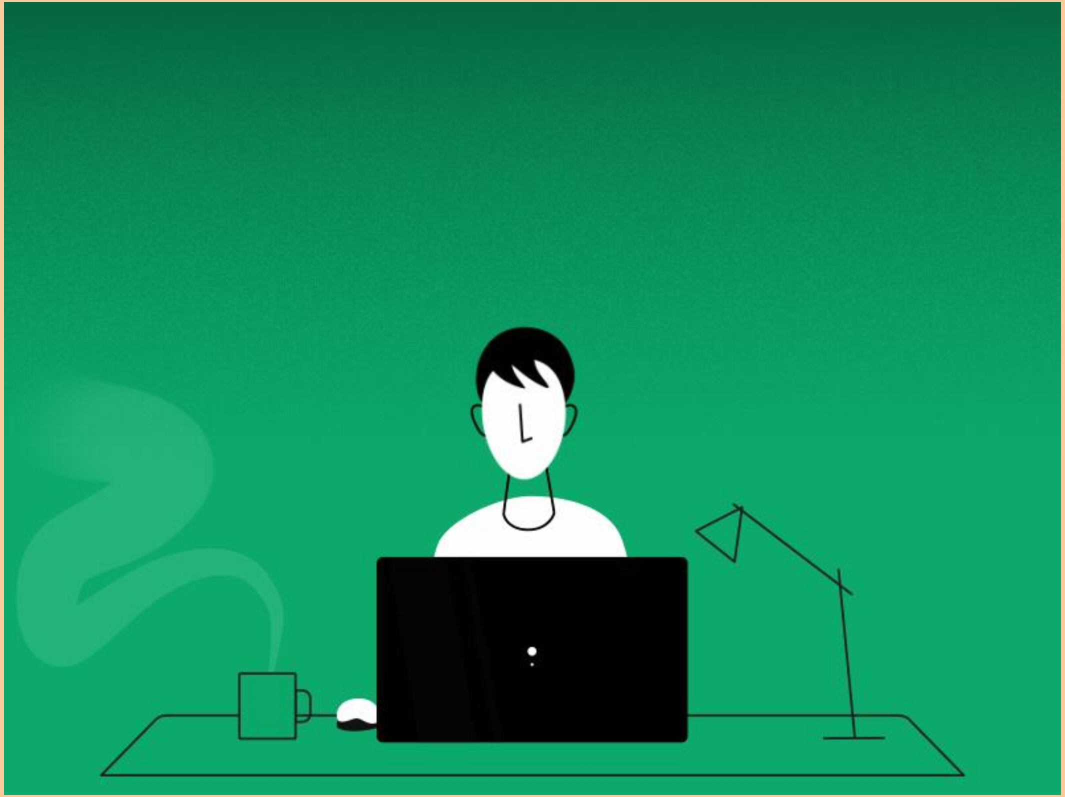
A **deeper dive** into the first step of a penetration test: reconnaissance.

Important!

The techniques we will learn throughout this unit can be used to break into networks and do serious damage to organizations' infrastructure. This is illegal when done without permission.

Therefore, do not take today's tools and techniques lightly.

Do not practice against computers you do not own or have written permission to be interacting with.



(Source)

What is Penetration Testing?

Penetration testing, often referred to as pen testing or ethical hacking, is the offensive security practice of attacking a network with the same techniques a hacker would use. The goal is to identify security holes and raise awareness in an organization.

Penetration Testing

While network administrators and security personnel do their best to harden their networks, it often takes an external entity to identify misconfigurations and subtle security holes.

Organizations hire pentesters to assess their security controls.

Pentesters find flaws in those controls, help the organization understand them, and provide recommendations about which vulnerabilities to prioritize and how to fix them.

Pentests are often administered by consultancies, which can take an “outside” view of a client’s networks.

Practitioners often refer to penetration tests as an **engagement**.

Penetration Testing

Pentesters, unlike hackers, receive permission from the security owner to carry out an engagement (the act of a penetration test).

Stages of Engagement

An engagement consists of five stages, similar to the stages of other offensive security practices we've looked at in past units:

01 Planning and Reconnaissance

02 Scanning

03 Exploitation

04 Post-Exploitation

05 Reporting

This Unit

Over the next three days, we will cover the first three stages of engagement:

01

Day 1: Planning

Defining the purpose and scope of the test, and conducting passive and active reconnaissance.

02

Day 2: Scanning

Once we have access to the organization's infrastructure, we can perform scanning and enumeration techniques to find valuable targets

03

Day 3: Exploitation

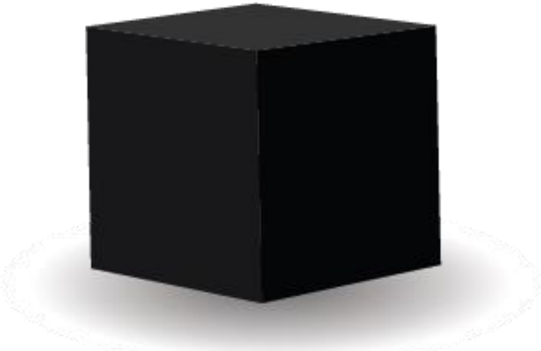
After scanning networks for vulnerabilities, we can execute the exploits that we know an organization is vulnerable to.

Types of Penetration Testings

Types of Penetration Testing

There are three types of penetration tests:

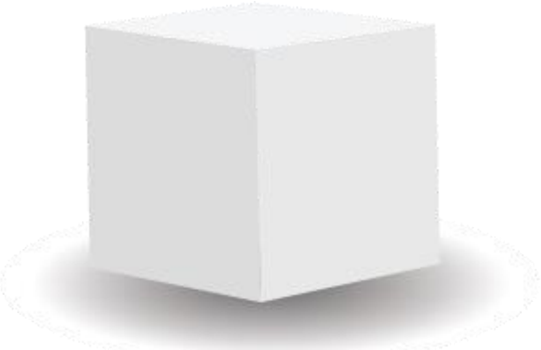
No View



Also known as

Black Box

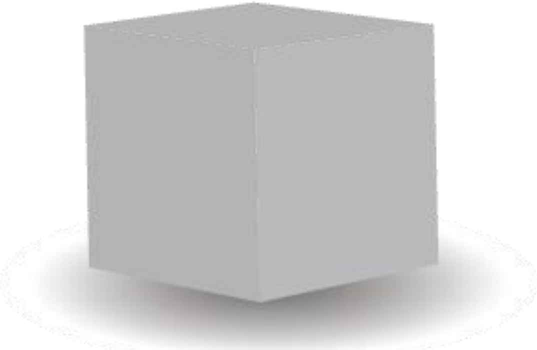
Full View



Also known as

White Box

Partial View



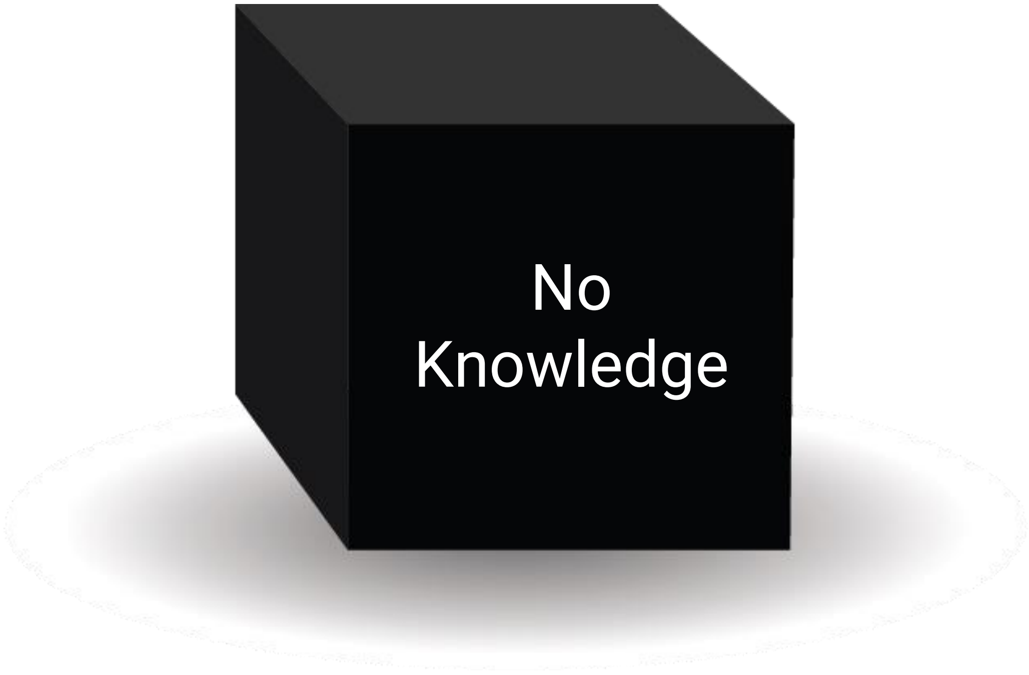
Also known as

Grey Box

No View Pen Testing

No view testing simulates a malicious hacker who has no prior knowledge of the target system and network.

- These testers are paid to learn and exploit as much as they can about the network using only the tools available on the public internet.
- For example, they may only know the company name and have to find various key resources, like IP ranges and access credentials, on their own.



Full View Pen Testing

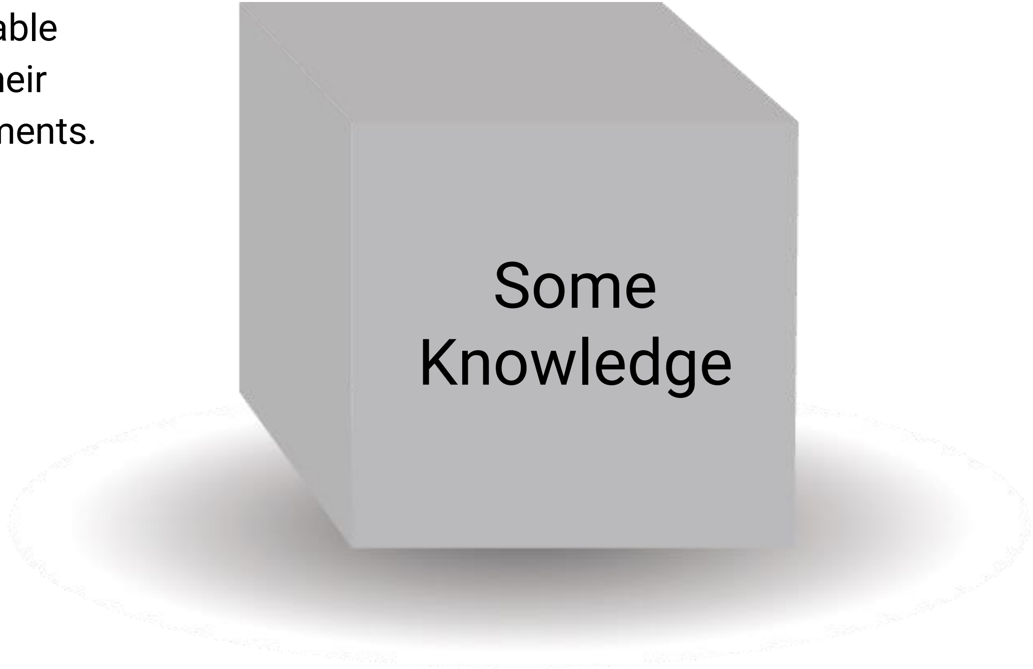
Full view penetration testers are given full knowledge of the system or network.

- This knowledge allows them to tear apart subtle security issues on behalf of their clients.
- These pen testing is most appropriate when a client wants a detailed analysis of all potential security flaws, rather than all exposed and visible vulnerabilities.
- Full view testers are given network diagrams, access credentials to the networks, system names, usernames, emails, and phone numbers.

Partial View Pen Testing

Partial view pen testing is performed by the in-house system or network admin.

Regardless of the scenario, the main deliverable for pentesters is a report that summarizes their findings and recommendations for improvements.



Planning

Planning

The specific environment that a pentest takes place in is determined before the penetration test occurs, in a planning interaction between the organization and the pen testing team.

(Source)

Planning

Businesses are not primarily interested in how attackers might gain access to their networks.

Instead, they are concerned with how an exploited vulnerability might impact their reputation, operations, and bottom line.

Scope and Purpose

Pentesters must work with clients to determine the **purpose** and **scope** of an engagement.

01 Purpose

Purpose is determined by the client's needs and concerns, and which assets the business is most interested in protecting.

02 Scope

Scope is based on which machines and networks are off limits.

Penetration Testing

Penetration testing is a competitive field to enter.

Pentesting requires ongoing skill development, and it is highly recommended that aspiring pentesters establish and maintain a personal lab environment to practice in.

Specific certifications are also desirable.

In the next activity, we will explore the vast field of certifications, focusing specifically on pentesting certifications.

Activity: Certification Research

In this activity you will research five pen testing certifications and answer questions for each:

- What is the purpose of each certification?
- Who is the certifying entity?
- What topics and skills does the certification cover?

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Reconnaissance

Passive and Active Recon

There are two types of reconnaissance: **passive** and **active**.

01 Active

Directly engaging with a target system.

For example, running a port scan directly on a server.

02 Passive

Trying to gain information about a target's system and network without directly engaging with the systems.

Pentesters can use the massive amounts of information that already exist on the web. For instance, third-party tools may have already scanned a system. We can use these third-party tools to get information without engaging directly with a system.

Huge amounts of both useful and superfluous information exist on the web.

The challenge is knowing what is important and how to extract it.

Reconnaissance

Offense informs defense.

Adversaries have become experts at extracting information from the internet. We need to become experts too, so we can defend against them.

Today’s reconnaissance will focus on external reconnaissance, also referred to as **open source intelligence (OSINT).**

OSINT

Since no view pentesters begin their engagement with very limited knowledge, they must use OSINT to gain as much available information about their target as possible.

- The information gathered in this stage plays a critical role in other phases of the engagement.
- For example: OSINT intelligence such as IP address blocks can be used to perform network scans to determine if a target is behind a firewall.

(Source)

OSINT

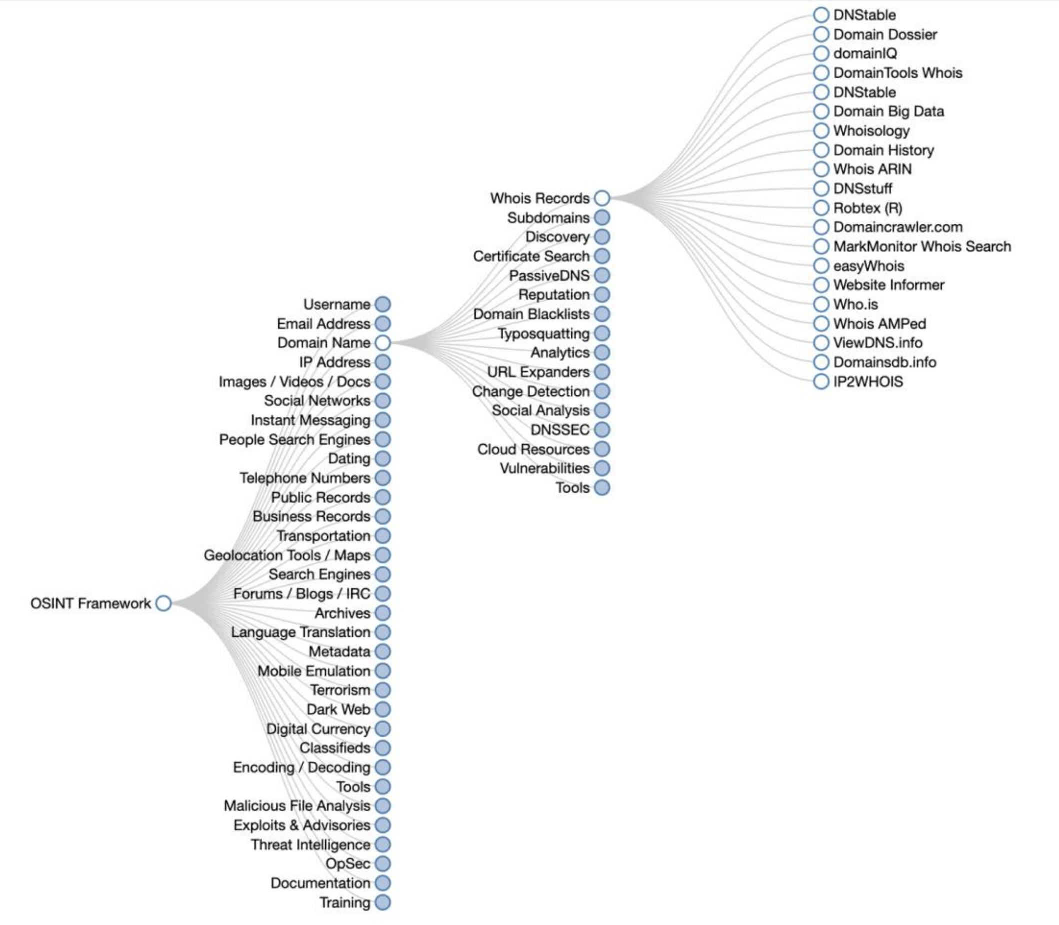
Other useful OSINT intelligence includes:

- Usernames
- Email addresses
- Phone numbers
- Domain names

WHOIS

We’ll use WHOIS databases to acquire OSINT intelligence for a DNS registrar and try to enumerate a target’s IP addresses.

- We’ll use the osintframework.com, a website that aggregates OSINT tools. These are free and used for information gathering across the web.
- Other websites may require paid registration. But you should be able to complete information gathering without paying for anything.



Remember!

Gathering information about a person or organization using the public domain is legal. Since OSINT involves gathering publicly available information, it is totally legal.

Using that information to gain access to systems that do not belong to you or you do not have permission to access is *illegal*, and a potential felony.

Remember!

For example, performing any of the following without the specific, written permission of the system's owner would be considered a felony:

01

Port scans

02

Brute force attacks

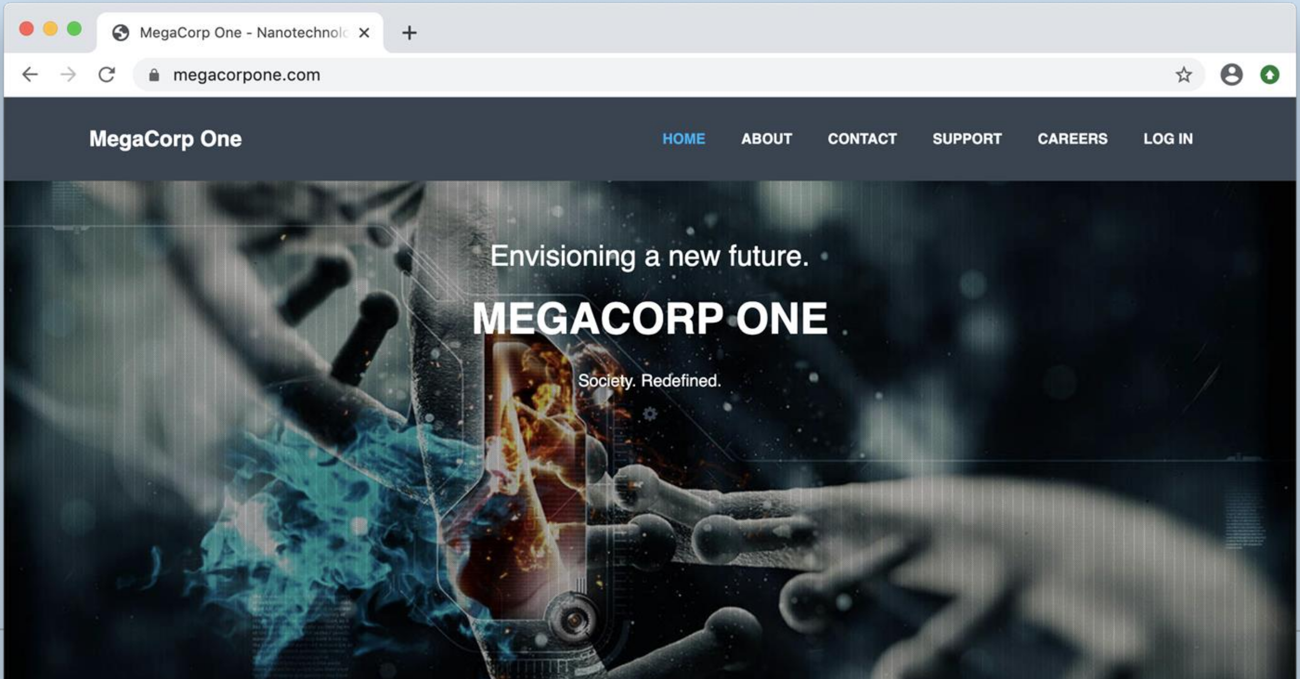
03

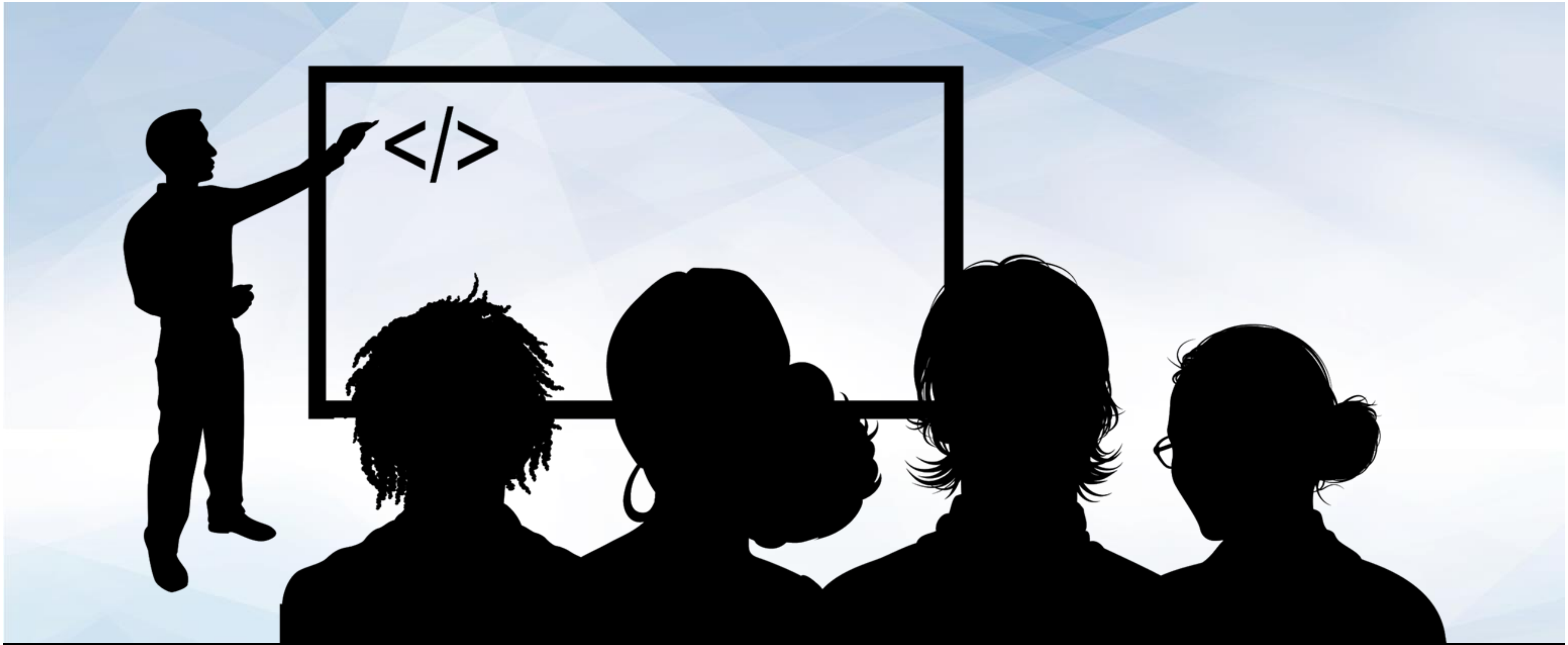
Social engineering

OSINT Demo

For this demonstration, we will use the fictional company MegaCorp One.

MegaCorp One is a fictional company created by Offensive Security. It was designed as a training tool to be used in their Penetration Testing with Kali Linux (PWK) training.





Instructor Demonstration

OSINT

Activity: DNS and Domain Discovery

In this activity you will perform DNS enumeration by viewing WHOIS record information.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

Google Dorking, Shodan, and Certificate Transparency

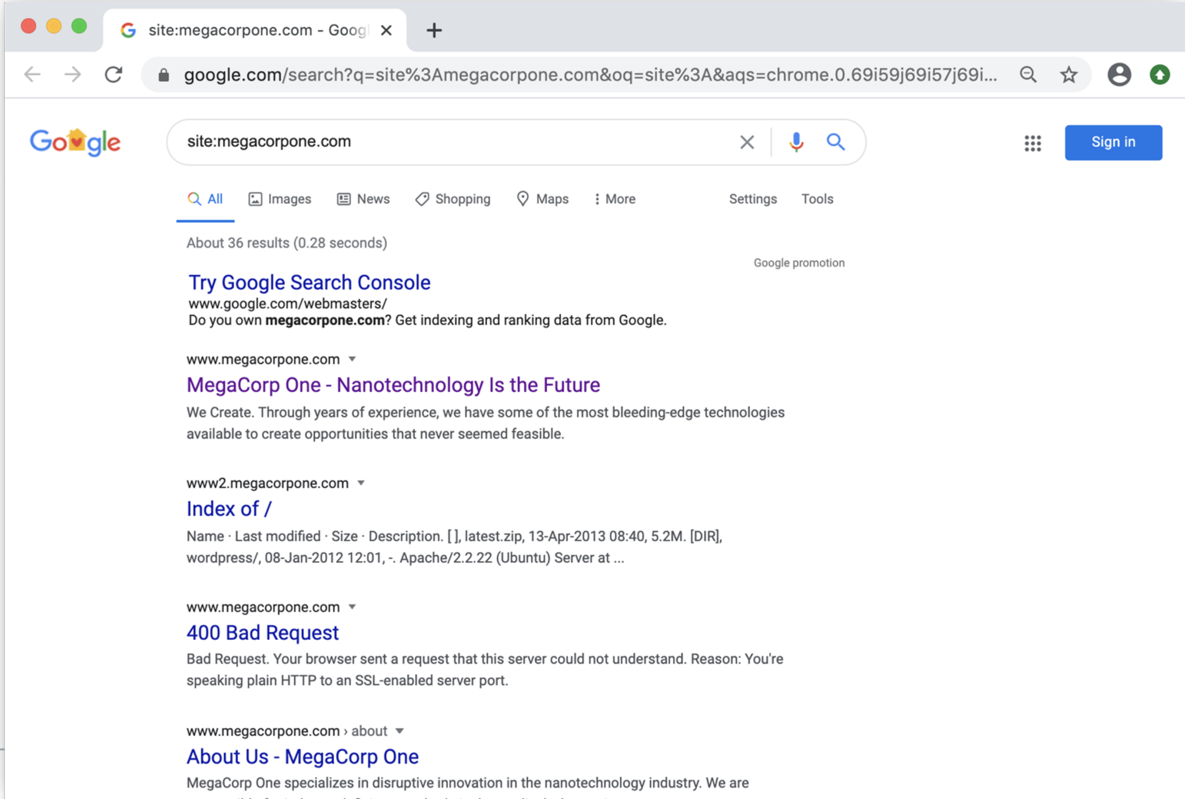
Now that we’ve learned why DNS domain discovery is useful for attacks and pentests, we will explore other TTPs that we can use in the reconnaissance stage of an engagement.

Google Dorking

also known as **Google hacking**, is a technique that leverages Google for OSINT and discovery of security holes in a website’s code.

Google Dorking

In this demonstration, we'll use Google search techniques to target MegaCorp One.



site:megacorpone.com - Googl
google.com/search?q=site%3Amegacorpone.com&oq=site%3A&aqs=chrome.0.69i59j69i57j69i...
site:megacorpone.com
Sign in
All
Images
News
Shopping
Maps
More
Settings
Tools

About 36 results (0.28 seconds)

Google promotion

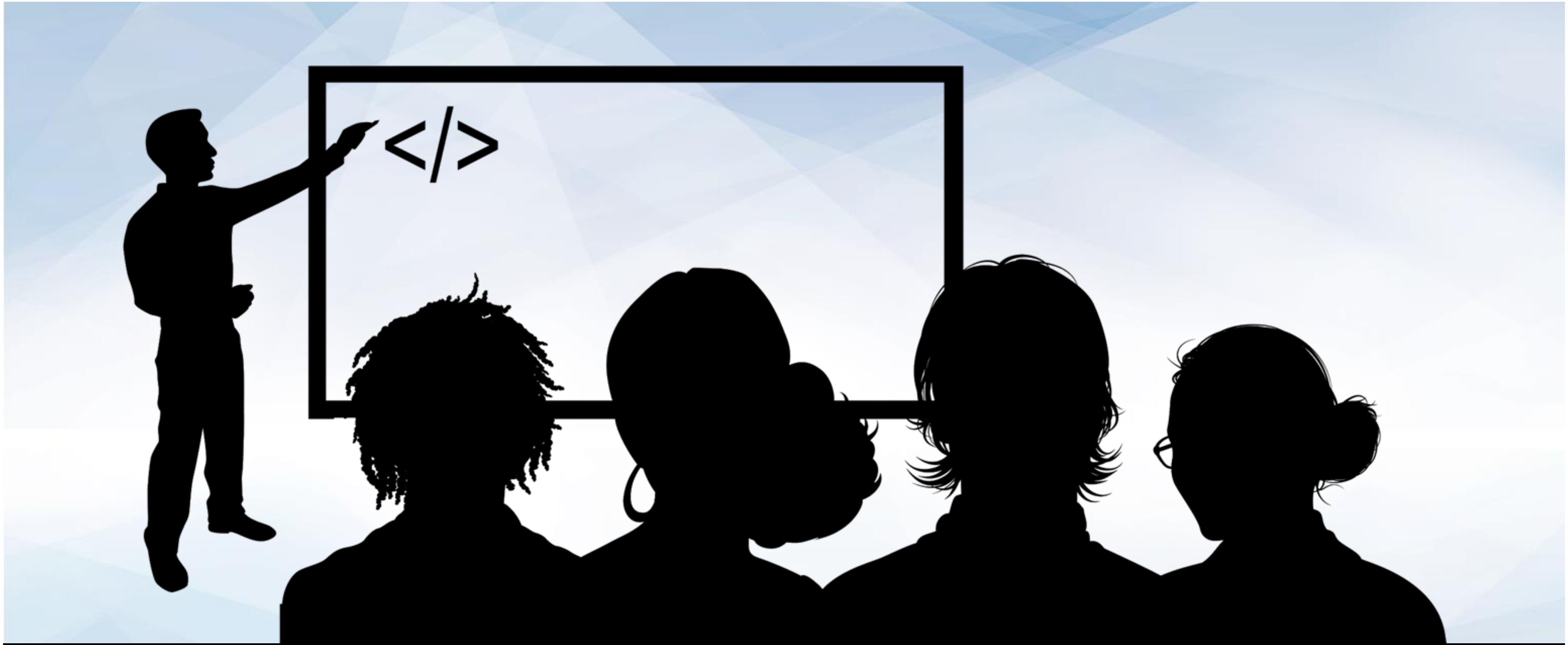
Try Google Search Console
www.google.com/webmasters/
Do you own **megacorpone.com**? Get indexing and ranking data from Google.

www.megacorpone.com
MegaCorp One - Nanotechnology Is the Future
We Create. Through years of experience, we have some of the most bleeding-edge technologies available to create opportunities that never seemed feasible.

www2.megacorpone.com
Index of /
Name · Last modified · Size · Description. [ ], latest.zip, 13-Apr-2013 08:40, 5.2M. [DIR], wordpress/, 08-Jan-2012 12:01, -. Apache/2.2.22 (Ubuntu) Server at ...

www.megacorpone.com
400 Bad Request
Bad Request. Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port.

www.megacorpone.com › about
About Us - MegaCorp One
MegaCorp One specializes in disruptive innovation in the nanotechnology industry. We are



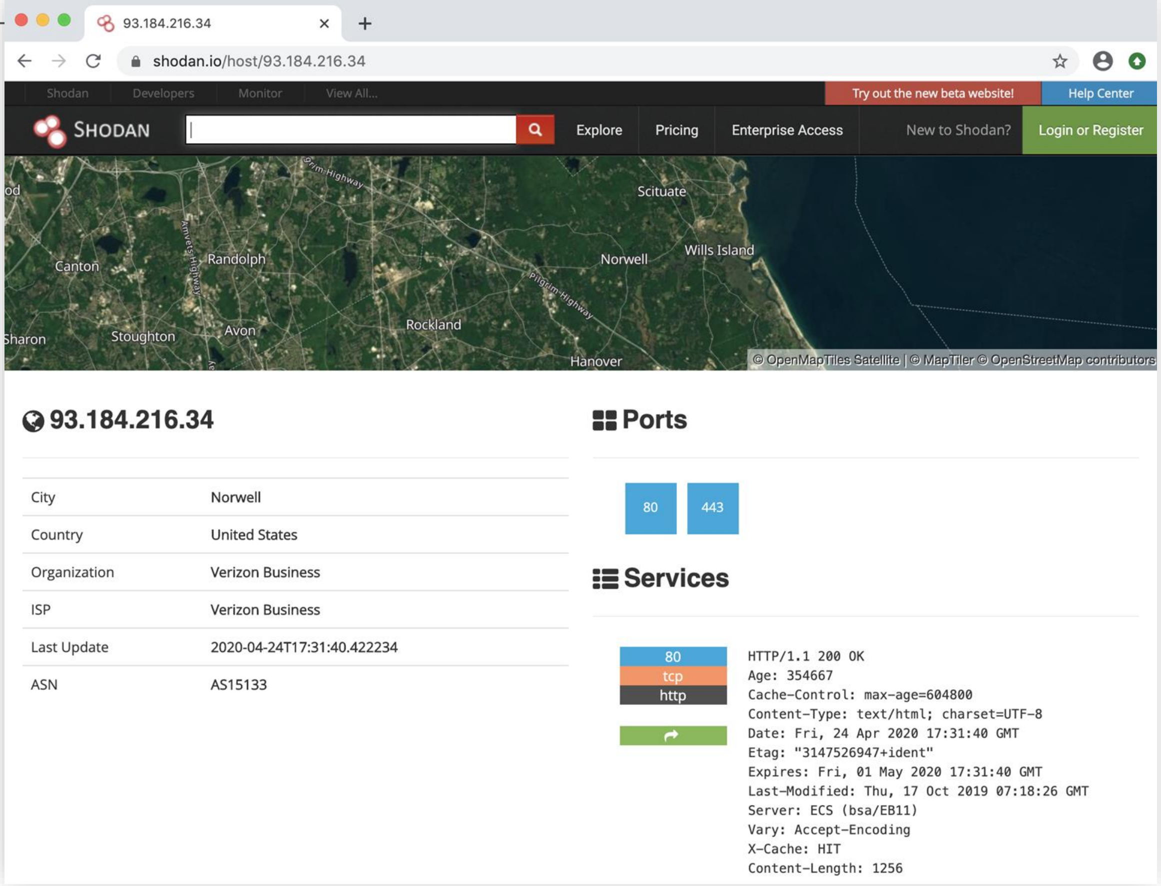
Instructor Demonstration

Google Dorking

Shodan

Another useful OSINT tool is Shodan, a search engine that scans the entire web and reports back all of its findings in the browser window.

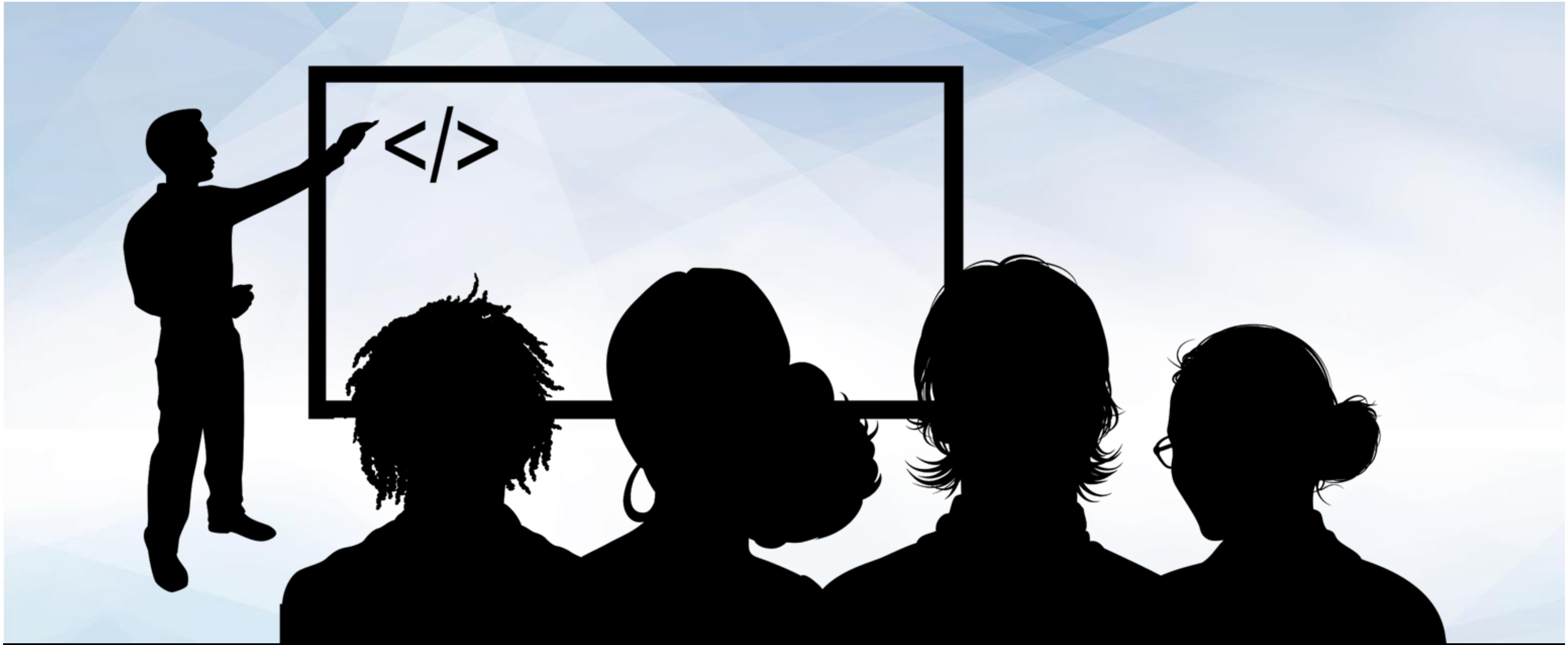
In the following demonstration, we'll use Shodan to find IP addresses.



93.184.216.34

City	Norwell
Country	United States
Organization	Verizon Business
ISP	Verizon Business
Last Update	2020-04-24T17:31:40.422234
ASN	AS15133

```
HTTP/1.1 200 OK
Age: 354667
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Fri, 24 Apr 2020 17:31:40 GMT
Etag: "3147526947+ident"
Expires: Fri, 01 May 2020 17:31:40 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (bsa/EB11)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256
```



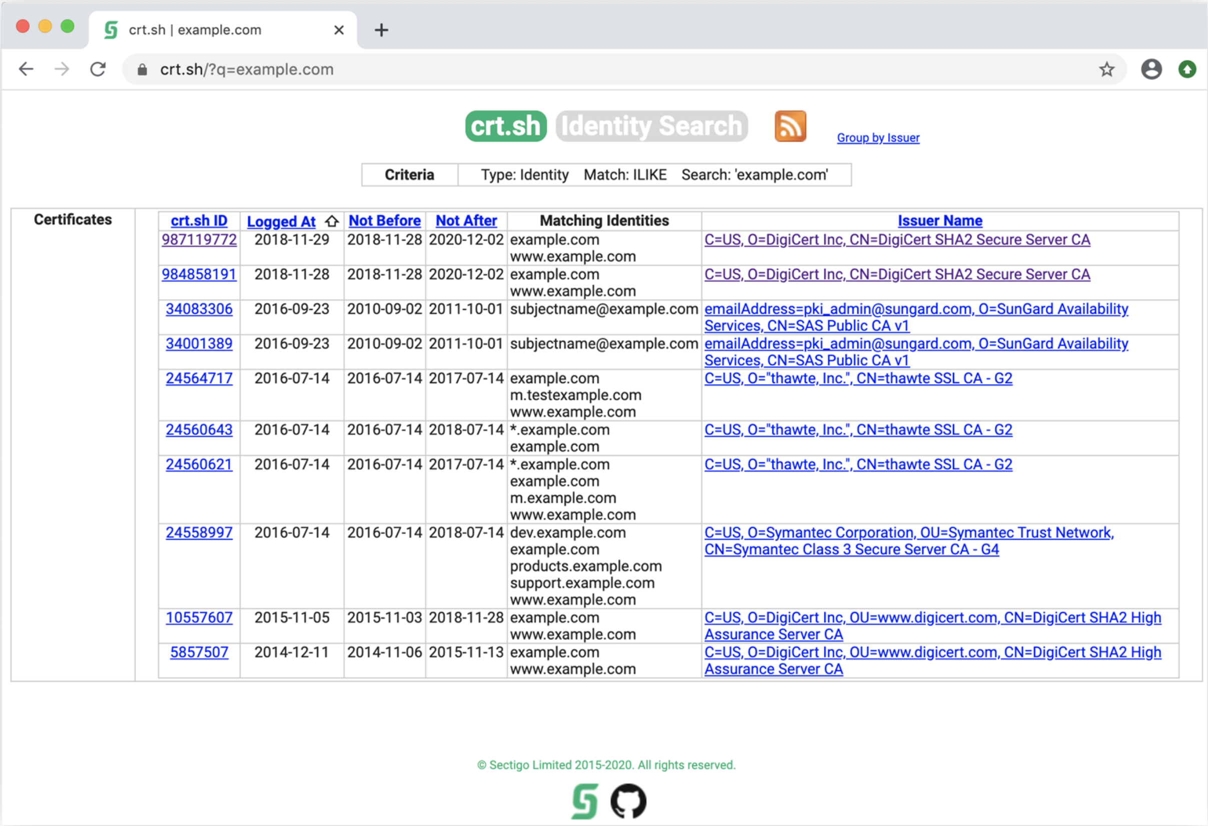
Instructor Demonstration

Shodan

Certificate Transparency

Certificate issuers publish logs of SSL/TLS certificates that they issue to organizations.

Attackers and pen testers can exploit this certificate transparency to search for subdomains.

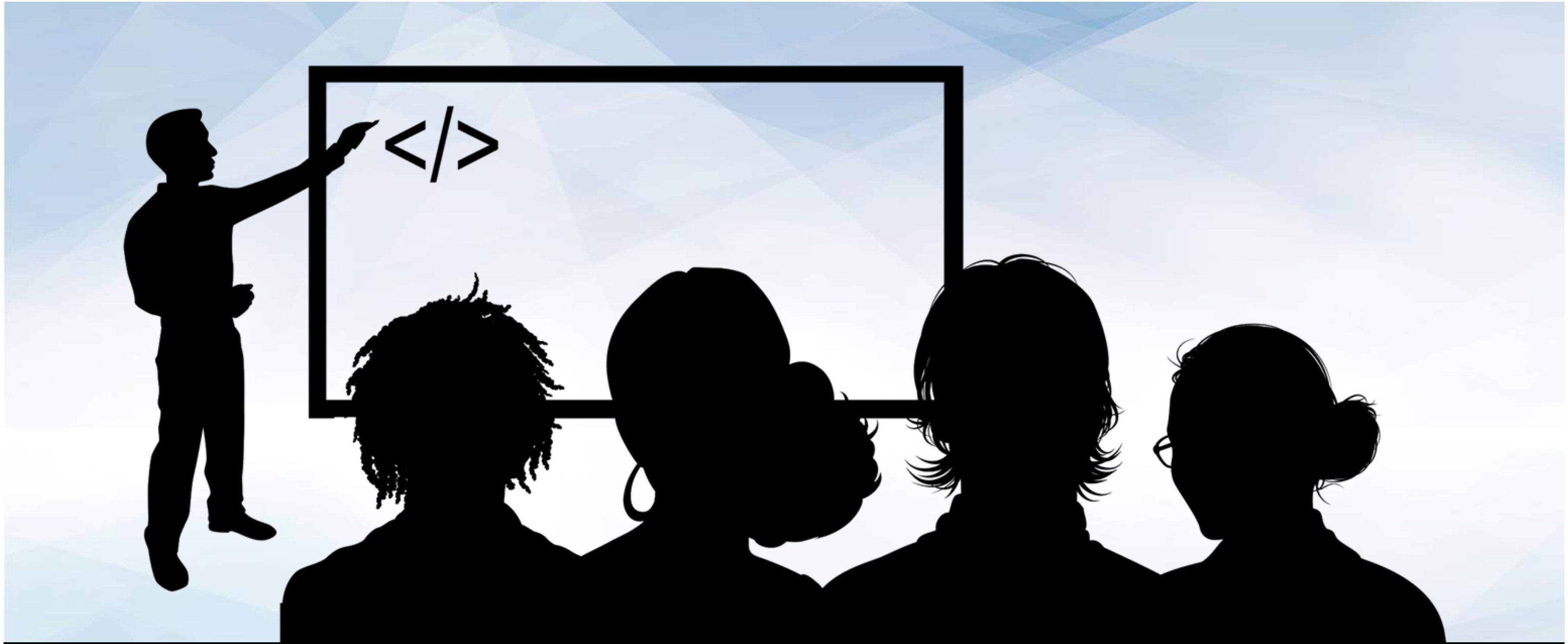


Criteria	Type: Identity Match: ILIKE Search: 'example.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Matching Identities	Issuer Name
987119772	2018-11-29	2018-11-28	2020-12-02	example.com www.example.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
984858191	2018-11-28	2018-11-28	2020-12-02	example.com www.example.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
34083306	2016-09-23	2010-09-02	2011-10-01	subjectname@example.com	emailAddress=pki_admin@sungard.com, O=SunGard Availability Services, CN=SAS Public CA v1
34001389	2016-09-23	2010-09-02	2011-10-01	subjectname@example.com	emailAddress=pki_admin@sungard.com, O=SunGard Availability Services, CN=SAS Public CA v1
24564717	2016-07-14	2016-07-14	2017-07-14	example.com m.testexample.com www.example.com	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
24560643	2016-07-14	2016-07-14	2018-07-14	*.example.com example.com	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
24560621	2016-07-14	2016-07-14	2017-07-14	*.example.com example.com m.example.com www.example.com	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
24558997	2016-07-14	2016-07-14	2018-07-14	dev.example.com example.com products.example.com support.example.com www.example.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
10557607	2015-11-05	2015-11-03	2018-11-28	example.com www.example.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
5857507	2014-12-11	2014-11-06	2015-11-13	example.com www.example.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA

© Sectigo Limited 2015-2020. All rights reserved.



Instructor Demonstration

crt.sh

Activity: OSINT Recon

In this activity you will perform initial information gathering recon of MegaCorp One’s network using Google dorking, Shodan, and certificate transparency techniques.

Suggested Time:
25 minutes

Recon-ng

Recon-ng is a web reconnaissance framework written in Python.

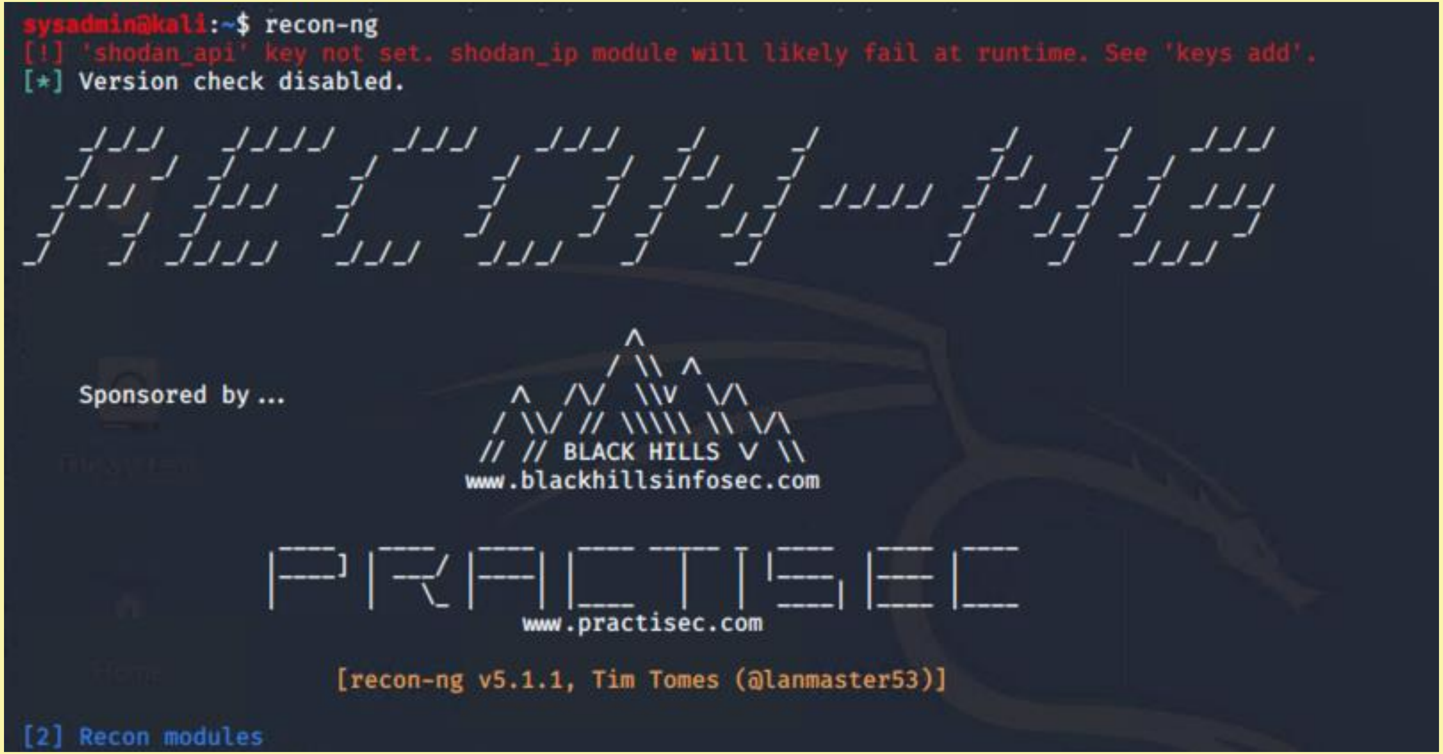
Recon-ng

Recon-ng is powerful, open source, and web-based, and works thoroughly and quickly. It includes the following features:

- Independent modules
- Database interaction
- Built-in convenience functions
- Interactive help
- Command completion

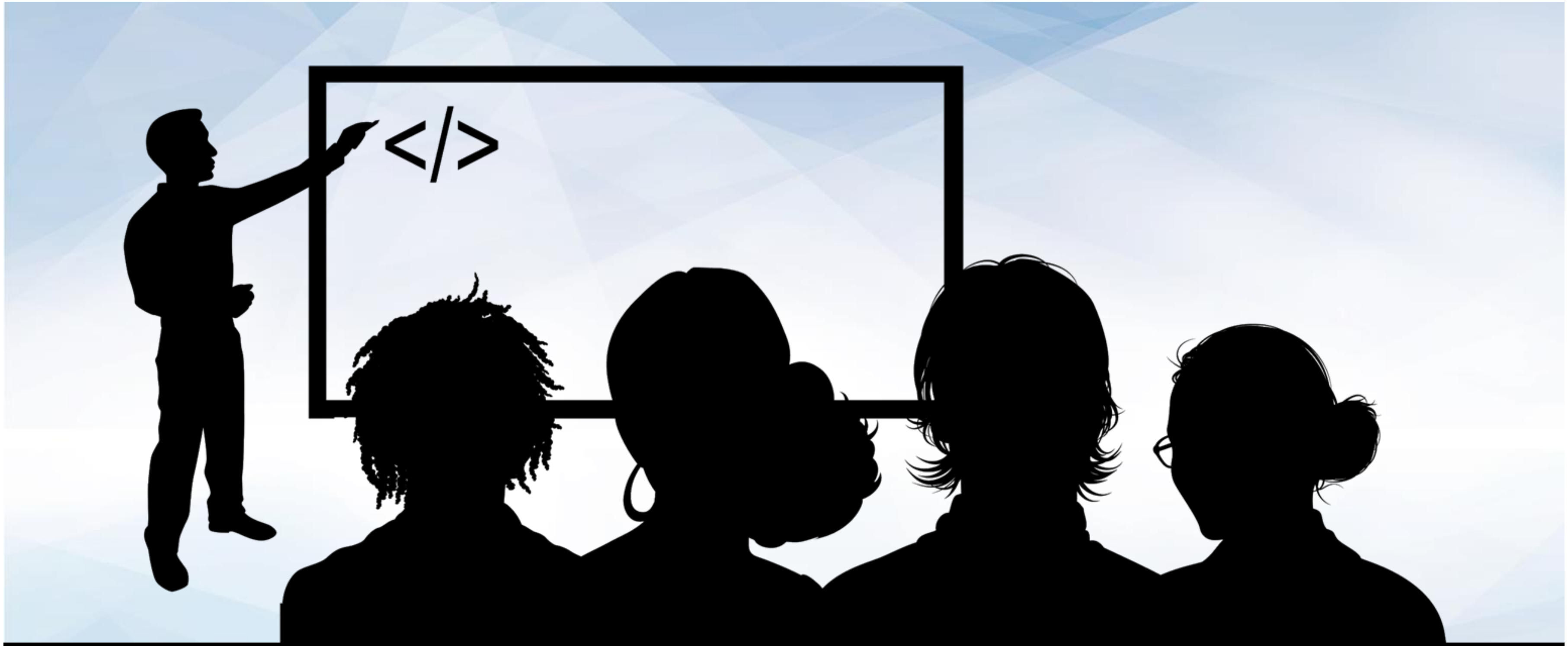
Recon-ng and Scripts

Many scripts and programs can be used to integrate OSINT tools into Recon-ng.



```
sysadmin@kali:~$ recon-ng
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See 'keys add'.
[*] Version check disabled.

    Sponsored by ...
                                        // // BLACK HILLS \/ \\
                                       www.blackhillsinfosec.com

                                           www.practisec.com

                          [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[2] Recon modules
```

Recon-ng ingests a lot of popular OSINT modules, allowing the results of multiple tools to be combined into a single report.



Instructor Demonstration

Recon-ng

Activity: Recon-ng

You will use the Shodan API and Recon-ng to test if your client’s domain server info is accessible with OSINT tools, then place your findings in a report.

Suggested Time:
20 minutes

Time’s Up! Let’s Review.

The End